GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO. *317
TO BE ANSWERED ON: 25.03.2021

INCREASE IN CYBER ATTACKS ON VITAL INSTALLATIONS

***317. SHRI SUSHIL KUMAR MODI:**

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether it is a fact that in last six months cyber attacks on the country's vital installations have increased;

(b) the number of cyber attacks and list of installations that have been attacked, State-wise;

(c) the amount of Budget that has been provided for cyber security in 2021-22; and

(d) the other steps that Government proposes to take to counter cyber attacks, the details thereof?

ANSWER

MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

(a) to (d): A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN REPLY TO RAJYA SABHA STARRED QUESTION NO. *317 FOR 25-03-2021 REGARDING INCREASE IN CYBER ATTACKS ON VITAL INSTALLATIONS

……

(a) and (b): The Indian Computer Emergency Response Team (CERT-In) is serving as national agency for responding to cyber security incidents as per provisions of Section 70B of Information Technology Act, 2000. CERT-In receives inputs from its situational awareness systems and threat intelligence sources about malware infections in networks of entities across sectors and issues alerts to concerned organisations and sectoral Computer Security Incident Response Teams (CSIRTs)for remedial measures.

Since last six months, during Covid-19 pandemic period, there has been a rise in scanning and malware infections towards networks of entities across sectors.

(c): For the financial year 2021-22, a total sum of Rs.416 crore has been earmarked for Cyber Security in Ministry of Electronics and Information Technology (MeitY).

(d): Government has taken following measures to enhance the cyber security posture and prevent cyber attacks:

i. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on regular basis.CERT-In has issued 451, 444 and 1039 alerts and advisories during the year 2018, 2019 and 2020 respectively to organizations and users for securing IT infrastructure and systems.
ii. Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.

iii. All the government websites and applications are to be audited with respect to cyber security prior to their hosting. Auditing of the websites and applications is conducted on a regular basis after hosting also.

iv. Government has empanelled security auditing organisations to support and audit implementation of Information Security Best Practices.

v. Government has formulated Cyber Crisis Management Plan (CCMP) for countering cyber attacks for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors. 10 workshops were conducted in the year 2020.

vi. Cyber security mock drills are being conducted regularly in Government and critical sectors. 6 such drills were conducted in 2020 covering 135 organizations across sectors including Power and Health.

vii. 24X7 Cyber Security Incident Response mechanism is in place at CERT-In

viii. 24x7 Security Monitoring Centre is in place at National Informatics Centre (NIC), for detecting and responding to security incidents related to NIC infrastructure and data centres. Additionally for enhancing Data Security, periodic security audits and vulnerability assessment of resources are performed followed by subsequent hardenings.

ix. **Capacity Building and Training**

- **CERT-In Trainings**: CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. During the year 2020, 15 training programs were conducted covering 708 participants.
- **Online Training in Cyber Security for Government officials** - MeitY is offering generic training (awareness level) and foundation training (advanced level) online in Cyber Security for officers of Central Government Ministries/Departments.

a. Generic Training (Awareness Level) :3879 officers/staff from 71 Ministries/Departments have attended.
b. Foundation Training (Advanced Level) :448 officers/staffhave successfully completed training.

- **Information Security Education and Awareness(ISEA)programme**A total of 68,251 candidates have been trained / under-going training in various

formal/non-formal courses in the area of information security through 52 institutions. 15,518 Government officials have been trained in various short term courses through direct/e-learning/ Virtual Instructor-Led Training (VILT) mode in the area of information security.

- **Cyber Surakshit Bharat (CSB) programme**: 18 batches of deep-dive cyber security training have been conducted in partnership with industry consortium. 698 CISOs/IT officials from Government, PSUs, Banks and Government organisations have attended the CSB programme.

x. **Cyber Security Testing and Certification by Standardisation Testing and Quality Certification (STQC) Directorate, MeitY**

a. Cyber Security Certification activities performed are as follows:
   - Common Criteria Certification – Product security testing as per ISO 15408. STQC being a certification body have common criteria recognition arrangement with other countries.
   - Information Security Management System (ISMS) - STQC operates third party ISMS certification scheme based on the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 standard and offers ISMS Certification services since November 2001 to its valued clients in India and abroad.

b. Cyber Security testing/evaluation/audit activities includes Web application security, Mobile Application Security, Vulnerability Assessment/Penetration Testing (VA/PT), End-point Devices security, Security Design/Architecture and Code Review, Security Process & Cloud Security Audit, etc.

xi. Government is operating the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

xii. Government has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats. Phase-I of NCCC is operational.

xiii. National Critical Information Infrastructure Protection Centre (NCIIPC) issues regular alerts, advisories and best practices to stakeholders from critical sectors.

****